Definitions Index:

Additional Resources:

- Federal Trade Commission Information Security Site
  www.ftc.gov/infosecurity
- Federal Trade Commission Privacy Initiative
  www.ftc.gov/privacy
- National Institute of Standards and Technology (NIST) Computer Security Resource Center
  http://.csrc.nist.gov
- OnGuard Online
  www.OnGuardOnline.gov
- Secure South Carolina
  www.secure.sc.gov
- State Budget and Control Board Policies
  http://cio.sc.gov/councilscommittees/aoc/policies.htm

Identity Theft and the Law

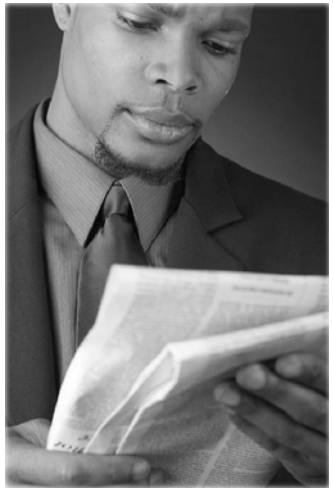
A Guide for Government and Businesses

Their **information**
Your **responsibility**

South Carolina Department of Consumer Affairs
3600 Forest Dr., Suite 300 Columbia, SC 29204
Local: 803.734.4200 Toll Free: 800.922.1594
Web: www.scconsumer.gov

The South Carolina Financial Identity Fraud and Identity Theft Protection Act

Identity theft is this nation's fastest growing crime. According to the Federal Trade Commission's Identity Theft Complaint Data Reports, over the past three years South Carolina has risen six places in the rankings of identity theft victims by state. To aid in combating identity theft in South Carolina, the South Carolina Legislature passed, and Governor Mark Sanford signed, the **Financial Identity Fraud and Identity Theft Protection Act** (The Act, The Law) (Act No. 190, 2008).



The Act provides several protections for consumers in the areas of security freezes, credit reports, records disposal, security breaches and more. The Act also places requirements on businesses and public bodies with regard to the collection, maintenance and disposal of consumers' personal information. All portions of the law, except the provisions regarding security breaches, become effective on December 31, 2008. The security breach provisions become effective July 1, 2009**.**

This brochure is meant to highlight important portions of the Act and not to serve as a substitute for reading the Act. References to portions of the laws amended or added by the Act are to the appropriate section number within the South Carolina Code of Laws. The complete Act may be found on the South Carolina Department of Consumer Affairs website at www.scconsumer.gov or at the South Carolina Legislature's website at www.scstatethouse.net.

Identity Theft and the Law: Q&A

Q: When my employees are finished processing documents that contain people's personal identifying information (PII), they put the documents in the recycling bin or trashcan. Is that ok?

A: No. *The law requires that the records be shredded, erased or that another method is used that ensures the PII is unreadable or undecipherable.*

Q: Do I notify the Department of Consumer Affairs only when 5,000 or more South Carolina residents are affected by a security breach?

A: No. *The requirement to notify the Department, and national credit reporting agencies, is triggered when more than 1,000 South Carolina residents are affected by your organization's security breach.*

Q: Are there any consequences for not complying with the Financial Identity Fraud and Identity Theft Protection Act?

A: Yes. *The Act provides several penalties including being fined by the Department of Consumer Affairs and sued by an affected person.*

Q: What can I do to assist my staff and organization with complying with the Act?

A: Plenty. *Take stock of the PII your organization receives or has on file and develop a data security plan, data disposal plan and security breach plan. Implement staff training so they are clear on the organization's policies and procedures regarding the protection of PII. As always, the Department of Consumer Affairs is available as a resource to answer questions and provide educational literature on the Act.*

Other Provisions Under the Act

■ *Seller/ Lender Credit Card Issuer (Section 37-20-120):*
Businesses that mail offers to receive a seller or lender credit card must verify a change of address if the application returned states an address that is substantially different from the address on the offer. A seller/ lender credit card issuer is prohibited from mailing out additional credit cards to a new address if the card is requested within 30 days of the address change, unless the change of address is verified by the issuer.

New Crimes:
Financial Identity Fraud (Section 16-13-510) and "dumpster diving" (Section 16-11-725), the rummaging or stealing of another person's household garbage for the purpose of committing identity theft or fraud.

Penalties:
The crime of "dumpster diving" can be either a misdemeanor or felony, dependant on willfulness. The crime of Financial Identity Fraud is considered a felony and punishable up to ten years of imprisonment and/or fines.

■ *South Carolina Law Enforcement Division (SLED) (Section 37-20-150):*
Provides for SLED to develop an identity theft victims database.

■ *Register of Deeds and Clerk of Court (Section 30-2-330):*
Unless required by law, persons preparing or filing documents with the register of deeds or clerk of court cannot put the following on the document: social security number, driver's license number, checking account, credit card or debt card number, etc. A violation is a misdemeanor with a $500 fine per violation. A register of deeds and a clerk of court shall place notices in their respective office as well as on the Internet regarding the restrictions above. The notice must be identical to that in section 30-2-330(C). An affected person may petition a court for an order compelling compliance if the register of deeds or clerk of court is not in compliance with this section.

Security Freeze

Section 37-20-160

Beginning December 31, 2008, South Carolina consumers can place a security freeze on their credit reports. When in place, the credit report cannot be accessed without the consumer's permission.

The freeze may be temporarily removed, or "thawed," at the consumer's request. The thawing can be for a specified time or a specific creditor and must be enacted within 15 minutes of the consumer's request.

There is **no cost** to place, thaw or remove a security freeze. The freeze does not apply to credit reports provided to government entities acting pursuant to a subpoena, court order, etc; child support agency; Department of Revenue; Department of Social Services when investigating fraud; etc.

To place a freeze on your credit, contact the following credit reporting agencies:

Equifax
www.equifax.com
800-685-1111 or TDD 800-255-0056
P.O. Box 105788, Atlanta, GA 30348

Experian
www.experian.com/freeze
888-EXPERIAN (397-3742) or TDD 800-972-0322
P.O. Box 9554, Allen, TX 75013

TransUnion
www.transunion.com
888-909-8872 or TDD 877-553-7803
P.O. Box 6790, Fullerton, CA 92834

Business Records Disposal

Sections 37-20-190 & 30-2-310

Persons conducting business in South Carolina and public bodies must properly dispose of records and items containing consumer's personal identifying information (PII).

A public body is defined as any department of the State, state board, commission, agency, and authority, public or governmental body or political subdivision, as well as any organization, corporation, or agency supported in whole or in part by public funds, including any bodies by whatever known name and quasigovernmental bodies of the State and its political subdivisions.

Personal Identifying Information (PII) consists of a consumer's first name or initial combined with their last name and unencrypted or unredacted data including the consumer's social security number or driver's license number or financial account number (includes credit card, debit card and security code) or other numbers or information that would allow access to the consumer's financial accounts.

Gramm-Leach-Bliley Act

The Federal Gramm-Leach-Bliley Act and the Safeguards Rule put safety requirements on "financial institutions" with regards to consumers' personal information.

A "financial institution" includes businesses that are "significantly engaged" in providing financial products or services, such as checkcashers, mortgage brokers, and real estate appraisers.

Requirements include developing a written information security plan and assessing and addressing risks to customer information in all areas of operation.

Businesses and public bodies must make the PII unreadable or undecipherable when disposing of records and remove it from hardware, storage media and other items before selling, transferring or otherwise disposing of the item.

- To a person providing the social security number to government.

Further, a public body:

- May not collect a person's social security number or six or more digits of the number UNLESS the body is (1) authorized by law or (2) the collection is imperative to the body performing its duties and responsibilities.

- When collecting a person's social security number or six or more digits of the number, must separate the number from the rest of the record, or as otherwise appropriate, so the number can be easily redacted pursuant to a FOIA request.

- At a person's request, must give a statement of purpose for collecting the person's social security number or six or more digits of the number and how it will be used.

- Can only use a person's social security number or six or more digits of the number for the purpose stated.

Social security numbers and other identifying information may be released by a public body under certain circumstances, including (Section 30-2-320):

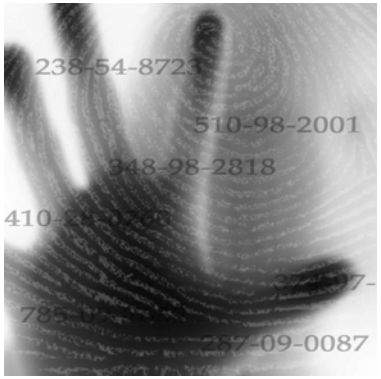
- Pursuant to a court order, subpoena, etc.
- For public health purpose.
- On a recorded document in county's official records.
- On document filed with court.

Social Security Numbers

Sections 37-20-180 & 30-2-310

Among other prohibitions, a public body and a person may not:

- Make available to the public a person's social security number or six or more digits of the number.
- Intentionally print or imbed a person's social security number or six or more digits of the number on a card required for access to a product or service.



- Require a person to transmit a social security number or six or more digits of the number over the internet UNLESS there is a secure connection or the number is encrypted.
- Require a person to use his/her social security number or six or more digits of the number to access the web unless a password is also required.
- Print a person's social security number or six or more digits of the number on materials mailed to that person UNLESS state or federal law requires it.

This portion of the law does not apply to the following scenarios, among others listed in section 37-20-180(B):

- Collection, use or release of a person's social security number for internal verification.
- To a person acting pursuant to a court order, subpoena or other legal process.

The Disposal Rule

Any business or individual who uses a consumer report for business purposes is subject to the Federal Disposal Rule. This includes debt collectors, attorneys, lenders and government agencies. The Rule requires that reasonable measures be implemented to ensure the proper disposal of information in consumer reports and records and prevent the unauthorized access to and use of the information.

The director of the public body or its information technology person must verify that all personal and confidential information is removed from computer items and items are sanitized in accordance with the Budget and Control Board standards and policies.

A business or public body is compliant if they hire a third party to destroy records in a manner compliant with the Act. The following businesses are **exempt** from this section:

- Bank or Financial Institution subject to, and in compliance with, the Gramm-Leach-Bliley Act.
- A health insurer subject to, and in compliance with, the Health Insurance Portability and Accountability Act of 1996.
- A consumer credit reporting agency subject to, and in compliance with, the Fair Credit Reporting Act.

Penalties for businesses:

- Private Cause of Action: actual damages, attorneys fees.
- Civil Action against businesses.
- Administrative Action pursuant to Title 37, Chapter 6.

Security Breach

Sections 1-11-490 & 39-1-90

Persons conducting business in this state and public bodies must notify South Carolina consumers when a security breach occurs.

A security breach is the unauthorized access to, and acquisition of, items containing PII and the illegal use of the PII has occurred or is likely to occur. Disclosure of the breach must be made within a reasonable, expedient time from the discovery or notification of the breach.

Consumers must be notified through direct mail, electronic means, telephone, notification of statewide media, or substitute notice. If notice of a breach is sent to more than 1,000 persons at one time, the business or public body must also notify the Department of Consumer Affairs and the national credit reporting agencies.

When a person is required to notify the Department of Consumer Affairs and credit reporting agencies of a security breach, the notice should include all of the following:

1. When the breach occurred.
2. When notice was given to affected persons.
3. Number of persons affected by the breach.
4. A copy of the notice sent to affected persons.

Penalties:

- Civil Action: damages, injunction, attorney's fees and costs;

Sample Security Breach Notification Letter

Date

Organization's Name and Address

Affected Person's Name and Address

Dear (Person's Name):
I am writing to inform you that our organization experienced (or discovered) a security breach on or about (date of breach or when breach was discovered). Unfortunately this has resulted in unauthorized access to your personal identifying information, specifically your (identify information that was or is reasonably believed to have been acquired).

(Organization Name) is taking this matter very seriously and has (describe steps taken to prevent further harm or access to the person's personal identifying information and indicate whether or not law enforcement and/or the Department of Consumer Affairs was notified of the breach). If you have any questions about this notice, please contact (name of contact person) at (contact's telephone number). You may also contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for information on steps you can take to defend yourself against identity theft.

Sincerely,

- Administrative fines of up to $1,000 per resident.

Financial Institutions are considered in compliance if abiding by the laws delineated in section 39-1-90(J).

Security Breach Notification:
Security Breach Notifications should be mailed to:

Legal Division
RE: Security Breach Notification
South Carolina Department of Consumer Affairs
P.O. Box 5757
Columbia, SC 29250

If you have any questions regarding security breach notifications, or the Act, please contact the Department at 803-734-4240.